UNIVERSITY OF OSLO
Faculty of Law

Privacy and E-Government

The Analysis of i2010 Action Plan

Candidate number:5
Supervisor:Prof Jon Bing
Deadline for submission:(09/01/2009)
Number of words:15542

By Ebenezer Paintsil

September 9, 2009

Privacy and E-Government

The Analysis of i2010 Action Plan

Candidate number:5

Supervisor:Prof Jon Bing

Deadline for submission:(09/01/2009)

Number of words:15542

By Ebenezer Paintsil

September 9, 2009

Contents

1 Introduction **1**
- 1.1 European Union (EU) Action Plan . . . 3
- 1.2 Research Problem . . . 3
- 1.3 Rationale and Relevance of the Study . . . 4
- 1.4 Structure . . . 4

2 i2010 Action Plan **7**
- 2.1 Overview . . . 7
  - 2.1.1 Inclusive e-government . . . 8
  - 2.1.2 Efficiency and Effectiveness . . . 9
  - 2.1.3 High Impact Key Services . . . 9
  - 2.1.4 Key Enabler . . . 10
  - 2.1.5 Electronic Participation . . . 11

3 Data Protection and Privacy Background **13**
- 3.1 Overview . . . 13
  - 3.1.1 What is Privacy? . . . 14
- 3.2 Ambit of Privacy . . . 16
  - 3.2.1 Overview . . . 16
  - 3.2.2 What is the Margin of Appreciation . . . 17
  - 3.2.3 What is Private Life . . . 18
  - 3.2.4 What is the Justification for Interference . . . 19
  - 3.2.5 Proportionality . . . 19
- 3.3 The Barriers of E-government . . . 20

4 Discussion **23**
- 4.1 Overview . . . 23
- 4.2 What is the Impact of the DPD on the i2010 Action Plan . . . 24
  - 4.2.1 Overview . . . 24
  - 4.2.2 Does the DPD Apply to E-government . . . 24
  - 4.2.3 Does the DPD Prohibit Intelligent Use of Data? . . . 26
  - 4.2.4 Interoperability . . . 31
  - 4.2.5 Data Security . . . 35
- 4.3 Does the i2010 Plan Shows Strong Privacy Concerns? . . . 39

4.4 The Need for Privacy Impact Assessment 40

5 Conclusion **43**

EU European Union

EEA European Economic Area

CCTV Closed Circuit Television

e-government Electronic Government

ICT Information Communication Technology

GISPPSIM Guidelines for Improving the Synergy between the Public and Private Sectors in the Information Market

DG Directorate General

IT Information Technology

EC European Commission

US United States

UK United Kingdom

DPA Data Protection Act

Data Protection Directive DPD

ECHR European Convention on Human Rights

ECtHR European Court of Human Rights

ICCPR International Covenant on Civil and Political Rights

UNCHR United Nations Commission on Human Rights

UN United Nations

DNA Deoxyribonucleic Acid

Http Hypertext Transfer Protocol

Https Hypertext Transfer Protocol Secure

PITAC President's Information Technology Advisory Committee

VAT Value Added Tax

eIDM Electronic Identification Management

PC Personal Computer

SIS Schengen Information System

ISO International Organization for Standardization

IEC International Electrotechnical Commission

ITIL Information Tecthnology Infrastructure Library

eTOM enhanced Telecom Operations Map

GAIT Guide to the Assessment of IT risk

Chapter 1

Introduction

Information and communication technology (ICT) has brought to us more efficient ways of storing, retrieving, transmitting and processing data. As a result of which we are witnessing various innovative application of ICT in both the public and private sector to ensure efficiency, effectiveness and customer or citizen convenience and satisfaction. Consequently, ICT has contributed to the rise in the use of "Code" in both public and private sectors with the anticipated objective of an improved service delivery and exercise of authority among others.

The European commission (EC) is one of the institutions which are concerned about how ICT can facilitate policy delivery in various areas of public administration. In the 80s the EC initiated the policy to ensure improved access to public information. The policy was known as the 'Guidelines for Improving the Synergy between the Public and Private Sectors in the Information Market (GISPPSIM) [1]. The Directorate General (DG) XIII was in charge of the implementation of this policy.

The public sector is the controller of citizen and government information which is valuable to the operations of businesses and enterprises. One of the core policy objective of GISPPSIM was to allow access to the information controlled by the public sector. The GISPPSIM was an attempt to stimulate the new information market in order to improve access to government held information . In this regard, quality information was made available to the private sector at a marginal cost to aid the day to day business operations. The public sector was regarded as information service provider, whose duty was among other things to sell information to the private sector.

[1] European Commission. Guidelines for improving the synergy between the public and private sectors in the information market. http://www.viw.or.at/intern/riand4.pdf, April 2006

The Directory General XIII has taken up new roles since its creation in the 80s. In 1986 it was revamped to take charge of the Telecommunication and Information Society Policy. Before 1993 the DG XIII in collaboration with other DG tackled the process of liberalization of the telecommunication sector defining an action plan for the development of the information society. In 2000 the DG XIII was organized and renamed (as Information Society & Media Directorate-General) once more to take up a new role under the eEurope Initiative [2].

One of the mandates of Information Society & Media Directorate-General is to implement the e-government policy. The policy is named i2010 action plan. This plan is expected to usher the European Union (EU) into a new era of more transparent public administration and service delivery to the citizens. It will once more rely on ICT to ensure the fulfillment of the policy objectives. Though both the former and the latter policies aim at transparent public administration, the e-government has a broader scope than the former DG XIII of the EC's GISPPSIM policy. The e-government initiative extends beyond the private sector or enterprise and just access to public information. It involves an all citizens' inclusive policy, effective and efficient services delivery, high impact services and interactive communication between government and citizenry.

While these kinds of policies that rely on ICT serve noble purposes, one of the setbacks is the effect of automation on our values system or rule of law in legislation. Certain aspect of policies which borders on law needs to be automated in order to derive the full benefit of the policy. This automation is done using computer programs. Policy automation allows rules of law in legislation, contracts, etc. to be implemented or expressed in computer programs [3]. Sometimes technical requirements and system design choices put limits on the law. These kinds of computer programs have been labeled differently by two of the famous authorities in the field of IT law, namely Lessig and Reidenberg.

Reidenberg calls these kinds of computer programs that implement policies or laws as lex informatica. Reidenberg argues that in a network environment or cyberspace, law and government regulations are not the only source of law. System design choices and the capabilities of the technologies in cyberspace impose rules on the people who use the network [4]. Lessig call these users

[2]Jean Monnet Professor Antonio Alabau. Understanding the e-government policy of the European union, pages 8-9. http://ec.europa.eu/idabc/servlets/Doc?id=18443, July 2003.

[3]Dag Wiese Stratum. Access to government held information, challenges and possibilities. http://www.viw.or.at/intern/riand4.pdf, February 1998.

[4]Joel R Reidenberg. Lex informatica: The formulation of information policy rules through technology. Texas Law Review, 76(3), February 1998.

cyberspace citizens [5].

1.1 European Union (EU) Action Plan

In an attempt to improve efficiency, to ensure more transparent public administration, and also to enjoy the full benefits of e-government, the EC in April 2006, came out with e-government action plan, an integral part of the i2010 initiative. This plan is expected to be fully implemented by the end of 2010. The plan is named i2010. The basic aim of this plan is to increase the number of cyberspace citizens by ensuring that every European citizens including the aged and disabled are motivated to use ICT to facilitate their day to day activities. This plan seeks to impact on the number of people who use the Internet and ICT technology. This will eventually give rise to the potential privacy incidents in cyberspace.

1.2 Research Problem

The EC i2010 Action Plan on e-government aims at ensuring that ICT and its applications will define the course of public administration in the years ahead. The plan is supposed to turn a new page in the history of public administration where more and more citizens will interact in cyberspace rather than in real space. The goal of this thesis is to investigate the potential impact of the EC Action Plan on individual privacy as more and more e-government systems are being implemented in fulfillment of this action plan. In this regard following questions will be examined

- Does the EU data protection directive (DPD) apply to e-government?
- Does the EU data protection directive prohibit intelligent use of data?
- What is the impact of EU data protection directive on interoperability?
- What is the impact of EU data protection directive on data security?
- Does the i2010 action plan show strong privacy concerns?
- Is there a need for privacy impact assessment as a benchmark indicator of the i2010 action plan?

[5] Lawrence Lessig. Code 2.0, volume 2. Basic Books, 2 edition, December 2006.

1.3 Rationale and Relevance of the Study

This thesis will examine the above question in order to understand how they impact on e-government. Generally, an electronic government system could contribute to the erosion of privacy and give the government undue power if it does not show strong privacy concerns in its design and implementation. There is the need for proactive measures in protecting individual privacy because it can be difficult to regain once it is gone. Privacy could serve as a powerful tool to check arbitrariness and disproportionate use of power in a democratic society. Personal data is a valuable asset and it protection will play a significant role in ensuring the balance of power between citizen and State [6]. A large scale usage, aggregation, exchange and data mining of personal data in e-government may have a negative effect on the balance of power between the citizen and the State and could result in privacy erosion.

Further, e-government system rely on trust and trust is imbued in security and privacy. Citizens could patronize e-government system if it provides them with the necessary convenience, security and privacy [7]. Privacy impact assessment could be relied upon to access the level of privacy in a e-government system. The i2010 action plan has major performance indicators which rate member states according to their progress and how close they are in achieving the objectives of the plan. It is not clear why privacy assessment is not part of the 52 performance or benchmark indicators.

Furthermore, the DPD set the lowest standard for data protection in the EU. It also tries to harmonize the data protection laws across the EU. It is therefore important to understand how these laws affect e-government. Does the directive serve as a barrier to e-government or does it supports the growth of e-government.

1.4 Structure

The next chapter examines the EC action plan in detail. We will consider the objective of the plan and the prominence of privacy and data protection in the plan.

The third chapter provides an overview of privacy and data protection and how e-government affects privacy. The objective of this is to help the reader to

[6] Xavier Huysmans. Privacy friendly identity management in e-government. SpringerLink, http://www.springerlink.com/content/a34758h15j085420/fulltext.pdf?page=1

[7] Asne Flyen Christine Hafskjold. Security and Privacy, page 2 www.teknologiradet.no, 2007.

properly appreciate the subject matter. It will also offer the reader the legal significance of privacy and why it is necessary to protect it from erosion through technological advancement. Various privacy cases will be discussed to throw more light on the subject matter.

The fourth chapter will mainly focus on discussing the research questions above. This will critically analyze the i2010 action plan on e-government with the aim of answering the research questions. It will focus on the impact of DPD on e-government, how other indicators such as privacy impact assessment may affect e-government patronage and the need to include them in the e-government performance metric or benchmark indicators.

The final chapter will offering opinions on the impact of i2010 on the privacy and whether or not the plan has adequate regard for privacy and data protection.

Chapter 2

i2010 Action Plan

2.1 Overview

E-government stands for electronic government or government online. It is the fusion of two words, electronic and government. According Donald F. Kettl, Government "*is an institutional superstructure that society uses to translate politics into policies and legislation*" [8]. Government is responsible for decisions making, development of substantive and procedures rules (bureaucracy), assigning roles (hiring and recruitment), and implementation of policies and performance evaluations of policies such as e-government and educational policies. In recent times, government is increasingly relying on ICT to fulfill its obligation to its citizens. E-government is an electronic tool that aids the government to fulfill it obligations to its citizens. It allows government to conduct its business on line or in cyberspace instead of the real space. E-government encompasses electronic workflow, electronic service delivery, electronic voting and electronic productivity .

In the 80s access to government information was key in ensuring transparent government. The contemporary times have witness new forms of demands for good governance and this includes more open, efficient, accountable and citizen centric government.

The main focus of e-government is to ensure efficiency in public administration by relying on ICT technology. E-government encourages greater public participation in government decision making and promotes a more open, more informed citizenry, cost effective, responsive and accountable government. With e-government the public can transact business with the govern-

[8]Thomas B Riley. e-government vs. e-governance, examining the differences in a changing public sector climate, page 6. May 2003

ment, get their Social Security checks, pay taxes, download documents (medical information), apply for governments' jobs, put in bids on contracts, fill out forms and applications and interact with their elected officials all in cyberspace or in an online environment.

What has become i2010 policy for e-government has a rather long history. It has evolved from the activities of the old DG XIII whose mandate was to promote information market in the early 80s. In 1986 the old DG XIII which was in charge of public administration was refocused and given additional responsibility of everything related to Telecommunications and Information Society [9]. It was renamed DG Information society. The DG Information Society together with DG Competition led the liberalization of the telecommunication market. Additionally, it put forward the action plan for the development of information society, (eEurope 2002) in 2000 and later on eEurope 2005. It is in this plan that the principles of e-government or online public administration were born. The focus on building ICT infrastructure and the liberalization of telecommunication market have to give way to a new realization of public administration and service delivery that depend on a new broad band ICT infrastructure.

The i2010 action plan is the EU's policy guideline on e-government. This guideline emerged from the eEurope initiatives and is the follow up of eEurope 2005. The guideline focuses on five main areas. They are inclusive e-government, efficiency and effectiveness, high impact key services, key enabler and citizen participation [10] [11].

2.1.1 Inclusive e-government

The EU is saddled with challenges such as ageing, access to Internet, lack of ICT skills etc. Inclusive e-government is to ensure that these obstacles are removed.

The inclusive policy is to ensure that no citizen is left behind. It targets the vulnerable and disadvantaged people in the EU who by virtue of their

[9] Understanding The e-government Policy of The European Union, pages 8-9,Antonio Alabau, Jean Monnet Professor, July, 2003, Working Document Reference, PTSI/24, http://ec.europa.eu/idabc/servlets/Doc?id=18443

[10] Commission of the European Communities. i2010 E-government Action Plan. Accelerating E-government in Europe for Benefit of all. http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id April 2006.

[11] European Commission Directorate General Information Society and Media. ICT for Government and Public Services. http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

state may be deprived from accessing e-government system. There is a need to bridge the digital divide between people who have access to ICT and those who do not. It was found that about 30% of Europeans do not use any e-government services. This 30% gap could be caused by the lack of ICT skill, readily available ICT infrastructure or affordable ICT services. Affordability is likely to impact unemployed citizens who may not be in the position to afford expensive ICT services or access. Ironically, such people who are excluded from e-government are those who are most likely to benefit from the e-government system . Furthermore, the policy also ensures that citizens are not discriminated against because of their disability or age. Multiple channels of access should be used to reach such citizens [12] [13].

2.1.2 Efficiency and Effectiveness

'Efficiency and effectiveness' is the second objective of the action plan. The main goal is to ensure efficient and effective service delivery. Efficiency may be the optimal mix of cost and benefits, while effectiveness is to obtain a certain level of service at the lowest cost. How long it take to deliver a service and how well we are able to satisfy our users may determine how this goal is achieved. It has ensured inter alia reduction in long queues and unnecessary delays in public administration, eliminated repetitive form filling and time consuming bureaucracy. The e-government system is expected to support effective decision making.

The direct benefits of this policy will be to improve the economy and governance since it will substantially reduce administrative cost, enhance transparency and accountability [12,13].

2.1.3 High Impact Key Services

E-government services are usually provided for the citizens of a particular member state even though certain services can be available for all member states. For instance since the EU supports effective competition and the single market, bidding for contracts can be available for all member states to com-

[12]Commission of the European Communities. i2010 e-government action plan, accelerating e-government in Europe for the benefit of all. http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id April 2006.

[13]European Commission Directorate General Information Society and Media. ICT for government and public services. http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

pete. It will be prudent for the development of e-government services that support such services to enable transnational access so that any member state can compete in the biding process.

The policy direction of high impact key services is to move from closed national access of certain key services to open transnational access to such services across the EU. Certain key services such as job search or, education could be made available across the EU. General services that facilitate greater citizen mobility could be made available to other Member States instead of limiting them to a particular State. This means the e-government has to be designed and built with large scale cross-border access in mind. Such system should be able to facilitate free movement, access to medical treatment, benefits and pensions, company registration and VAT refunding for businesses and education across the EU [10,11]. .

2.1.4 Key Enabler

Interoperable ICT systems are systems that can communicate with each other. Such systems need not to be identical or built on the same platform but should provide an interface that enable communication. E-government systems are built on different platforms and in different government department with different design and implementation schemes. For effective e-government such systems have to work together to meet the demands of the citizens, businesses as well as the public service or the administration. To prevent repetitive processes and duplication of data, effective e-government systems need to work together or inter operate.

The key enabler is an attempt to ensure effective e-government system through interoperability. It defines a system that will facilitate Interoperability of various e-government systems or subsystems. Such systems should be able to allow communication between e-government services running in different departments. The system should allow secure transfer of information or delivery of high impact services from administration to administration, administration to businesses and citizens both within and between countries in the European Union. It should be able to sustain a secured communication between services, departments, regions and EU countries.

Not only this, but also , access to e-government system needs to be open. Citizens from one Member State should be able to access high impact services from another Member State online with little or no constraint. Secure electronic identity and signature systems will be an important facilitator of this objective since they enable or boost online transactions. They allow authentication and identification of an individual in online environment to enable

them to access online resources. The action plan proposes electronic identities for all EU citizens instead of paper identity cards. This will facilitate efficient and effective identification.

Another key enabler is open source software. Open source software has source codes available for free. This means that the software can easily be altered to meet the need of a government department. Departments which have similar needs can share the same system and when the needs change the software can be easily altered to meet the new requirements. The cost associated with open sources is the risk of the responsible owner. Since the code is open people who use the code are responsible for any demand that may be associated with the code. On the other hand, government will be able to reduce cost since open source software are usually free or have less restrictive licenses requirements. However, governments will have to bear the risk associated with open source software such as maintenance and liability of error. [14] [15].

2.1.5 Electronic Participation

The citizens of EU are increasingly becoming less interested in politics. The election turnout has not being encouraging. The goal of electronic participation is to find a way of boosting citizen's interest in politics. To involve ordinary people in politics and policy making and making the decision making processes easier to understand through the use of ICT [12],[13]

[14]Commission of the European Communities. i2010 e-government action plan, accelerating e-government in Europe for the benefit of all. http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id April 2006.

[15]European Commission-Directorate General Information Society and Media. ICT for government and public services. http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

Chapter 3

Data Protection and Privacy Background

3.1 Overview

Privacy is one of the cornerstones of many democracies, yet difficult to define. In some democracies the protection of privacy is enshrined in the constitutions, others have general laws that expressly embody privacy protections. In the US for instance, privacy is regarded as a constitutional right [16]. Though privacy is not explicitly found in US constitution the Bill of Right establishes constitutional right and privacy may qualify as such [17]. European countries in general apply human right and human dignity approaches to privacy which may fall outside their respective constitutions.

Privacy depends on the normative values of a state. For instance Lessig [18], one of the authorities in privacy in the US suggests that personal data should be regarded as intellectual property that can be traded for profit. This is contrary to the Europeans which places emphasis on human dignity. It underscores the fundamental normative difference and the level of regard the EU has for privacy vis-a-vis the US. It also contradicts the normative neutrality concept expressed by Gavison [19].

[16] Daniel E Smith. The right to privacy, the rights and liberties under the law page 1. http://www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/glenn404.htm, April 2004

[17] David Bender and Larry Ponemon. Binding corporate rules for cross border data transfer, page 124. Rutgers Journal of Law and Urban Policy, 3:2, 2006.

[18] Lawrence Lessig. Code 2.0, volume 2. Basic Books, 2 edition, December 2006.

[19] David Bender and Larry Ponemon. Binding corporate rules for cross border data transfer, page 154. Rutgers Journal of Law and Urban Policy, 3:2, 2006.

Privacy in US is also sector specific and has no general applicability [20]. This situation in US is partly due to the general mistrust of government led regulations. Privacy provisions are scattered in many statutes and act. The EU however, has general law that protect personal data and oversight body that ensures compliance.

The EU has very stringent rules for privacy and data protection as compared to the US. This high level of regard for data protection in the EU has led to the issuance of "a world order" for protection of personal data. DPD article 25(2) [21] requires a third country (countries outside the EU/EEA) to have adequate data protection law in other to allow transfer of personal data from the EU to that country. This adequacy criterion is imbued in the principle of consent, data integrity, choice, purpose specification, necessity, and data security and so on.

Notwithstanding, this level of importance attached to personal data and for that matter privacy has led to a special agreement between the EU and the US in an apparent attempt by the EU to enforce or impose their law on the US. This agreement is known as the Safe Harbor agreement. The Safe Harbor agreement ensures that organizations in the US adhere to the tenets of the EU data protection laws. The agreement is only between the US and the EU. The significance of safe harbor is to allow organizations in the US whose operations require import of personal data from the EU to interact with the EU, so long as they meet the Safe harbor requirements.

Countries other than the US need to satisfy the high adequacy criteria in order to import personal data from the EU. So far only few countries such as Argentina, Switzerland and Canada are able to meet the high adequacy standard the EU has set.

3.1.1 What is Privacy?

Privacy is a vague word and actually difficult to define. The Black Law dictionary attempts to define privacy as a "*condition or state of being free from public attention to intrusion into or interference with one's acts or decisions*". It underlines two forms of privacy, the autonomy privacy and informational privacy. The autonomy privacy is the ability of an individual to control his or her personal activities or intimate personal decisions without outside interference, observation or intrusion. This means that an individual should be shielded from the

[20] David Bender and Larry Ponemon. Binding corporate rules for cross border data transfer, page 154-156. Rutgers Journal of Law and Urban Policy,3:2, 2006.

[21] Eu data protection directive. http://www.cdt.org/privacy/eudirective/EU_Directive_.html October 1995.

external world but only allow access when it suits her or is required by the law.

Privacy is also informational according to the Black law dictionary. Informational privacy is an individual's right to determine the extent to which information about oneself is communicated, especially sensitive data such as health information, political opinions, ethnic origin and so on. Thus information privacy is about the management of personal information.

In the 1890s, Louis Brandeis together with Samuel Warren illuminated the concept of privacy by defining privacy as individual's "*right to be left alone*" [22]. Warren and Brandeis also the fathers of privacy in the US, suggested that privacy was the most cherished of freedoms in a democracy, and advocated for its inclusion in US Constitution. It was argued however that privacy was already a constitutional right in the US.

They proposed that privacy is an independent legal norm and is embodied in the right to be left alone. Privacy does not depend on any other interest apart from the privacy itself, the right to be left alone.

This meaning of privacy was however challenged by Dean Prosser in the counter thesis on privacy. In Prosser's view privacy protects social norms or interest and is a composition of other values. Privacy is a social interest or the values the society places on protecting mental tranquility, reputation and intangible forms of property. Thus privacy is not an independent value as Warren and Brandeis seems to suggest but dependent on social norms such as mental tranquility and reputation. Is the right to be left alone the same as the right to protect one's reputation? Is the right to be left alone the same as the right to protect one's mental tranquility? Is the right to be left alone the same as the right to protect intangible forms of property? In Prosser's view these are separate interest that is not protected by the Warren and Brandeis's blanket concept of privacy [23].

What kind of interest is being protected by privacy? Warren and Brandeis may not be wrong after all as they assumed that the term "*privacy*" itself is complete and adequate to describe any interest being protected or threatened.

Robert Ellis Smith, editor of the Privacy Journal one of authoritative publication in the world on the individual's right to privacy, defined privacy as "*the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of*

[22] Electronic Privacy Information Center and Privacy International. Privacy and Human Right 2002, An International Survey of Privacy Law and Development, volume 1. Butterworths, 13 edition, 2002

[23] Edward J Bloustein Stanley I Benn. Philosophical dimensions of privacy, An Anthology. Cambridge University Press, 1984

disclosures of personal information about ourselves."

Basically, privacy has four main legal dimensions identified by physiological, relational, informational and territorial [24] [25] [26]. Physiological privacy concerns the autonomy or the right to protect ones physical self from invasive procedures such as genetic tests, drug testing and cavity searches. The relational privacy concerns with the autonomy or the right to the protection of correspondence such as emails, telephone conversations and so on. Thirdly, informational privacy is about autonomy or the protection of personal data. In the EU information privacy is regulated by Data Protection Directive. Finally, territorial privacy is concerned with the protection from intrusion into the domestic and other environments such as the work and public space.

3.2 Ambit of Privacy

3.2.1 Overview

The philosophy of privacy discussed above seems to suggest that privacy is a very imprecise concept with many definitions and unlimited scope. In this section we examine whether privacy is absolute right or not and if not how does the legal provisions help to set the limits of privacy. We examine the article 8 of European Commission on Human Right (ECHR) to understand the obligations or ambit of the provision.

Like any other right, privacy is not an absolute right and legal provisions usually safeguard the extent to which the right to privacy can be exercised. They determine the kind of right protected by privacy and the circumstances under which such rights could be exercised. These safeguards are not always explicit in various privacy conventions and statutes. The article 12 of International Covenant on Civil and Political Rights (ICCPR) and article 17 United Nation Convention on Human Rights (UNCHR) do not explicitly express the limit to which the right to privacy could be exercised. Though the main focus of these conventions is not privacy they have articles on data protection, and therefore may qualify as privacy conventions. On the other hand article 8 of ECHR is quite explicit on the extent to which the right to privacy could be ex-

[24] Ronald Leenes Bert-Jaap Koops. Code and the slow erosion of privacy. 12 Mich. Telecomm. Tech. L. Rev., 115, 2005

[25] Council of Europe The European Convention on Human Rights. ROME 4 November 1950 and its Five Protocols, STRASBOURG 20 January 1966. EU, January 1966.

[26] Electronic Privacy Information Center and Privacy International. Privacy and Human Right 2002, An International Survey of Privacy Law and Development, volume 1. Butterworths, 13 edition, 2002

ercised. The ambit of privacy could serve as an adequate tool in our quest to understand the privacy concept.

The understanding of article 8 of ECHR will better deepen our understand of right to privacy. In doing so we analyze the essential objects of article 8 [27] listed below

- Doctrine of the margin of appreciation
- Private life
- Justifications for interference
- Proportionality

3.2.2 What is the Margin of Appreciation

Another ambit of privacy is the doctrine of the margin of appreciation. It establishes that privacy is limited by the normative values of member states.

The margin of appreciation refers to the power of a judge in a contracting state to assess the circumstance surrounding a human right case base on the normative values of a state in exercising his discretion. The principle of the margin of appreciation is also the latitude of discretion allowed in a manner in which standard conventions are implemented, taking into account the normative values of a state. It follows that the decision of a judge in privacy matters will be limited by the normative values of the state. The margin of appreciation does not only set limits on privacy but it helps to safeguard the sovereignty of a State and also justifies the fact that a national judge is in a better position to assess the concrete circumstance of a case than an international judge.

The greatest challenge to the margin of appreciation is the potential abuse of the discretion. Yutaka Arai-Takahashi suggests that the limitation clauses (article 8(2)) could serve as the remedy to potential abuse of discretionary powers [28]. In relation to privacy, the exercise of discretional powers must be done

[27] 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[28] Yutaka Arai-Takahashi. Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR, page 3-10. Intesentia, 2002.

in accordance with the national law, it must be necessary in a democratic society and must pursue one of the legitimate rights of article 8(2) of ECHR. Margin of appreciation also has the tendency of impacting negatively on setting common standard for international human right.

Margin of appreciation is developed from case law and not the provisions of article 8 of ECHR.

3.2.3 What is Private Life

The ECHR article 8 protects individual against *"arbitrary interference by public authorities"* in his or her private life. What is the right to private life and where do we place the limit on private life. Does private life extend beyond the domestic sphere to work place, public places or embrace interpersonal relationship. We examine these in the light of the following cases, Peck v. UK (2003) and Niemietz v. Germany (1992).

Geoffrey Dennis Peck, is a United Kingdom (UK) national who lived in Essex. On 20 of August 1995 Peck attempted to commit suicide by cutting his wrist with a knife. He was unaware that he had been filmed by a closed circuit television (CCTV) camera installed by Brentwood Borough Council. The operators of the CCTV only observed an individual in the possession of a knife and alerted the police. The police arrived at the scene where they took the knife and detained Peck under Mental Health Act 1983. He was examined by a doctor and later released without any charges.

On the 9th of October the footage of the incident was released by the council to the public without masking Peck's face. The footage and the picture of the incident were published by various media houses some without specifically masking Peck's face.

On 23 May 1996 Peck applied to the High Court for leave to apply for judicial review concerning the Council's disclosure of the CCTV material. His request and a further request for leave to appeal to the Court of Appeal were both rejected. The case finally ended up with European Commission of Human Rights and the complaint was about the disclosure of the CCTV footage to the media and lack of an effective domestic remedy

The ECtHR held that disclosure of footage to the mass media without appropriate safeguards constitute a disproportionate and unjustified interference of the applicant's private life and violates article 8 of the ECHR. What is significant in this ruling is the limit of private life according to ECHR article 8. It seems that private life is not bounded by geographical location. The court's focus was on the right to be left alone rather than the location of the incident.

Private life can be lived in public sphere [29].

Another important case to consider is Niemietz v. Germany. Niemietz was a lawyer. In 1985 a judge Miosga, a district court judge received an offensive telefax signed by one K.W and sent by "AK-BL Freiburg" from the Freiburg post office. The court instituted criminal proceeding against K.W for insult. The court ordered investigation into the case. In the course of the investigation the court issued the search and seizure warrants of any documents found, inter alia, in the applicant's office which might aid in revealing the identity of K.W since the content of the letter was forwarded to the applicant address [30].

The ECtHR commission held that the search constitute violation of private life and that respect for private life comprised to a certain degree the right to establish and develop relationships with others. The notion of "private life" should not exclude professional or business relationship. The significance of this ruling is that private life extends beyond home to business premises

3.2.4 What is the Justification for Interference

The exercise of privacy right in the EU is regulated by ECHR article 8(2). It requires that exercise of privacy right can be limited or interfered with by law, necessity in democratic society, by the interest of national security, public safety, or economic well being among others. There should be a careful balance in how these safeguards are enforced. The thin line between these safeguards and the privacy protection is crucial in understanding privacy. How should these safeguards be enforced without infringing individual privacy? This balance is achieved through the principle of proportionality, reasonability, and non arbitrariness

3.2.5 Proportionality

Proportionality is a balancing act between computing interest. In balancing the computing interest, the considerations in favor of a course of action is placed on one side of a balancing scale and those against are placed on the other side. Rational people weigh the considerations and come up with a decision that follows the outcome of the balance. Proportionality in e-government will balance the interest of data subject against the interest of government in processing the

[29] ECJ. Judgment in the case between peck v united kingdom. http://www.echr.coe.int/eng/Press/2003/jan/Peckjudeng.htm, January 2003.

[30] ECJ. Case of Niemietz vs. Germany. http://www.bagger-tranberg.dk/EU-ret/Filer_homepage/Niemietz_vs_Germany.pdf, December 1992.

data.

Proportionality appears a few times in the DPD article 11(2). The use of proportionality has been inferred from other provision of DPD and other relevant human right conventions. However, it is one of the important principles in the determination of human right cases in the EU. Proportionality has become the basic principle of interpretation of the European Convention on Human Right [31]. It one of the principles which is mentioned explicitly in the Treaty on the European Union Article 5(4).

Most of the core principle of data protection could be determined with the aid of the proportionality principle. The excessive processing of personal data, the extent of the personal data processed, the purposes for data processing could be determined with the proportionality principle. The DPD article 6 could serve as a measure of proportionality.

Applying the proportionality principle requires that the measure is suitable and reasonably likely to achieve its objectives. The adverse impact of the measure is worthy of legal protection and justified in the view of the objective pursued.

3.3 The Barriers of E-government

The e-signature, e-commerce and data protection directives (hereafter key enabler directives) are supposed to resolve the legal obstacles to e-government according to the breaking the barrier to e-government project report [32]. For example, the formal legal requirements of administrative laws such as preference for manual signature to electronic signature, could serve as a barrier to e-government. Such formal legal requirements could be resolved by the implementation of these directives.

Unfortunately, the implementation of these directives have not entirely met the key enabler requirements anticipated in the i2010 action plan. The implementation of these directives has produced rather mix results as recognized by the breaking the barrier to e-government project.

The breaking the barrier to e-government project is the EC sponsored project which investigated the various obstacles to e-government. The program is in

[31] Professor J.H.H.Weiler, Proportionality: An Assault on Human Rights?, Jean Monnet Working Paper 09/08, http://www.jeanmonnetprogram.org/papers/08/080901.pdf

[32] Breaking Barriers to eGovernment, Overcoming obstacles to improving European public services Modinis study Contract no. 29172 http://www.egovbarriers.org/downloads/deliverables/1b/A_Legal_and_Institutional_Analysis_of_Barriers_to_eGovernment.pdf page 30-33

response to the requirements of the i2010 action plan. The overall goal of the project was to identify and explore the barriers to e-government progression in Europe and suggest organizational, technical and legal solutions to overcome these obstacles. This will go a long way to ensure the realization of the i2010 action plan key enabler policy objective. One of the objectives of the key enabler policy is to ensure that enabling legal framework is in place for successful implementation of e-government.

The project identified administrative law and traditions as one of the main legal obstacles to the progress of e-government in the EU. The immediate solution to this barriers is the modernization or adaptation of the administrative laws of member states to the requirements of technology through the implementation of the key enabler directives. The report suggested that the implementation of the key enabler directives has not successfully adapted the administrative laws and traditions of EU member states to meet the requirements of e-government. The implementations of these directive has underestimated the peculiar needs of administrative law which are necessary for e-government.

The legal reforms in the ICT field give an indication of modernization of certain aspect of public administration laws. For instance the e-commerce and e-signature directives provide the enabling legal framework for e-government and public administration in areas such as the recognition of electronic signature and electronic document. The objective clauses of the e-signature directive is to support the use of electronic signatures and to contribute to their legal recognition, the e-signature directive article 1. The legal equivalence of electronic signature obstacle is effectively resolved by the electronic signature directive. Similarly the e-commerce directive ensures legal recognition of electronic document, the e-commerce directive article 1(2). However the same cannot be said of the data protection directive.

In my view these legal reforms in the ICT fields both resolved and created additional barriers to e-government. The additional barriers created may not caused by implementation problems of the key enabler directive but the inherent requirements and objectives of the directives themselves. The data protection directive especially has a mixed impact on e-government. It seems to provide legal remedy against unlawful administrative practices rather than modernization of administrative laws. It could serve as a powerful tool to check arbitrariness and disproportionate use of power in public administration. It plays significant role in regulating the balance of power between citizen and state [33]. For instance, administration laws and traditions permit sharing of information across departments which may be prohibited by the data pro-

[33] Xavier Huysmans. Privacy-friendly identity management in e-government SpringerLink, http://www.springerlink.com/content/a34758h15j085420/fulltext.pdf?page=1

tection directives. Some states even permit the sale of personal information to the public as in the case of Robertson v City of Wakefield Metropolitan Council and Another 2001 EWHC Admin 915 LTL 16/11/2001 TLR 27/11/2001 (2002) 2 WLR 889 [34]. In this case, the Representation of the People Act 2000 (England and Wales) mandates the Electoral Registration Officer to disclose the full electoral register for commercial use upon payment of the appropriate fee. It was held that the administrative provision is inconsistent with article 8 of the ECHR and data protection act 1998. The DPD also ensures that data controllers put in place adequate security protection for the protection of personal data DPD article 17.

The DPD could have significant impact on interoperability which is the major requirement for the i2010 action plan's key enabler policy (see 4.2.4, 2.1.4). Interoperability relies on data sharing but the DPD prohibits unauthorized sharing of personal data.

This may calls for the possible review of the DPD in order to implement the policy. Unfortunately, reviewing the DPD to pave the way for the key enabler policy is likely to affect the e-government patronage. Reviewing the DPD would limit the power of citizens since privacy protection serves as checks on government. Furthermore, e-government patronage rely heavily on trust [35] therefore high level of privacy is paramount in building the trust in e-government system.

In effect privacy protection could be regarded as one of the greatest barrier to e-government.

[34] http://www.doughtystreet.co.uk/hrarp/summary/index.cfm?iStartRow=300&sSortBy=dtCaseDate&sOrder=ASC

[35] Asne Flyen Christine Hafskjold. Security and Privacy, page 2 www.teknologiradet.no, 2007.

Chapter 4

Discussion

4.1 Overview

Technological innovations usually come with their own legal challenges. No doubt, e-government is not an exception. Privacy, the absence of paper based documents and signatures, confidentiality and reliability issues will impact on the successful implementation of e-government system. The solutions to these challenges often rely on the legal equivalent of the offline regulation for online environment or in creating sector specific legal regulation to meet the new demand. Some jurisdictions generally adhere to the principle that, what applies to offline applies to online. Legal provisions of the offline world can be applied and upheld in the online environment. This will ensure clarity, consistency and legal certainty.

The Swiss legal system seems to emphasize this equivalence principle in their e-government report. The report states, "*The online world is not disconnected from the legal one, and many laws adopted long before the creation of the world-wide web still apply to online transactions. E-government projects must in particular comply with statutes more specific to the field, such as the general principles of administrative law and procedure (especially rules of inter-service information exchange), data and private sphere protection law, administrative transparency law, and, when applicable, intellectual and industrial property law, contract law and private international law*" [36]

On the other hand, there are very fine details which offline traditional legal rules are incapable of regulating because of certain inherent characteristics of the online environment and therefore require regulation change in certain

[36]Corien Prins. e-government, a comparative study of the multiple dimensions of required regulatory change page 11. Electronic Journal of Comparative Law, 11.3, December 2007

areas of e-government such as e-voting, e-procurement and privacy etc. E-voting for instance may require a handwritten signature to be replaced by an electronic signature. In the EU such new legal requirements of e-government could be addressed by the existing directives, such as DPD, e-signature directive etc. However, these directives may not be sufficient to meet the requirements of e-government or they may be an obstacle to the growth of e-government. In the light of these the subsequent sections will analyze the impact of the i2010 action plan on privacy by discussing the research questions 1.2 above.

4.2 What is the Impact of the DPD on the i2010 Action Plan

4.2.1 Overview

The data protection directive came into being at a time when e-government was not prominent as it is today. The DPD basically focuses on individual privacy and does not consider certain vital requirements of e-government such as interoperability. As a result the DPD could serve as a barrier to the development of e-government. This section discusses how the DPD affects or promotes e-government in the areas such as data security, interoperability among others.

4.2.2 Does the DPD Apply to E-government

The DPD protects data subjects from privacy abuse by data controller or processor. The Directive regulates the activities of data controller. Therefore the identity of the data controller is paramount in applying the DPD directive. Where it is impossible to identify the data controller, the DPD directive is likely to be ineffective. While identification of data controller in a small organization may seem obvious but the same cannot be said of an institutional superstructure such as government. Division of labor is not usually as prominent in small organizations as it is in big ones.

It follows that the question of whether or not the DPD apply to e-government will depend on the meaning of data controller and whether it is possible to identify a data controller in e-government. The possibility to identify a data controller in processing personal data on behave of the government will make the DPD directive applicable to e-government. The DPD article 2(d) defines

a data controller as a legal entity or a person who determines the purposes and means of the processing of personal data [37]. Also any legal person from whom the personal data originates for transmission from one location to another could be considered as data controller according to the DPD recital 47.

Ultimately, any legal person, agency or authority who determines the purpose and the means of data processing is a data controller. In government however, such legal person, entity or authority is not always distinct. The purpose and the means of processing are not always determined by a single entity. It is possible that the purpose and the means of data processing may be determined distinctively by different government agencies. The wording 'jointly' in this provision seems to carry the meaning of collaboration between two or more entities. It would be impossible for such government agencies to achieve meaningful results without some form of collaboration. On the other hand, since the interpretation of the DPD is usually dependent on the overall objective of a provision rather than the wording, it could be possible to determine a data controller in this context without placing much emphasis on the collaboration between the government agencies or departments.

Who has the authority to determine the objective of data processing in an organization superstructure such as government could also be determined from characteristics of such organization. Since government is hierarchical in structure and information flows from top to bottom it would be possible to find such a public authority or the entity responsible for determining the purpose of data processing. In such organization those lower in the hierarchy act on behave of those higher in the hierarchy. The wording 'public authority' in the DPD article 2(d) seems to suggest that any natural person or entity which legally act on behave of another could qualify as a data controller. In effect those entities or legal persons lower in hierarchy would eventually become the data controllers.

Data controller can also be identified during data transmission or by national law or regulation. Departments who are responsible for transmission of data from one location to another may be the data controller. Also national or Community laws or regulations could be relied upon to determine who is the data controller as stated in article 2d. Article 2b allows data controller to be determined by national law or Community law, regulation or specific criteria. This provision will be very useful in e-government where policies are usually backed by law or regulations.

[37] controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

We can therefore conclude that the DPD apply to e-government.

4.2.3 Does the DPD Prohibit Intelligent Use of Data?

Normalization is a technical means of removing data redundancy from databases. Normalization helps to avoid storing the same data in more than one database tables in order to prevent update anomalies. Most online information systems have databases support. Databases consist of tables which store the actual information. The tables in the database have to be designed to remove redundant information in order to save storage space and also make the database more effective in terms of time spent in retrieving information [38].

To achieve this aim, data from different department can be combined using so called primary and foreign keys. A primary key is a unique key or data that identifies a record or a set of data. The foreign key serves as a link that connect a unique primary key such as personal number or social security number to redundant or dynamic data such as login time in order to reduce redundancy and to prevent update anomalies. In normalization, we start with logically inconsistent table. The table is then split into two and primary and foreign keys are assigned to them. The primary key is attached to the static data table and the foreign keys are attached to the dynamic data table. The primary and the foreign keys are used to create a relationship between these two tables in the database. When this setup is complete the unique primary key can be used in several database tables without the need to repeat the name and address the primary key links to. This means by referencing the primary key the name and address can be known and dynamic or redundant data about an entry in the redundant information table can be known.

The following example will illustrates how normalization works. University of Oslo has student web which allows students to register for a semester course, check results among other things. The home page displays data, which consists of items such as department, semester fee paid completed semester registration, semester receipt sent, study programme, class, status and right to study. It also consists of student name, address, the name of the university etc. These items are called fields in database. Suppose the department field stores the department name and changes each time a student register for a course in a particular department. The Semester fee paid field stores data about when a student pays his or her fees and changes whenever a new payment is due. We can observe that some of the fields are dynamic or redundant and others are more or less static. The dynamic fields are those that change regularly such as Semester fee paid field etc. The student name, the study programme and the

[38] http://databases.about.com/od/specificproducts/a/normalization.htm

university name are static fields since they barely change. The initial database table for university of Oslo studentweb may have the following entries in table 4.1.

Table 4.1: Unnormalized entry

name	school	Study	Class	Status	Right	dept	fee paid	registration	course
John Haakon	Uio	ICT Law	2008 autumn	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
John Haakon	Uio	ICT Law	2008 autumn	Active	Plan confirmed 13.06.2009	ICTLaw	2009	2009	thesis
Andy Morrison	Uio	ICT Law	2008 autumn	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
Andy Morrison	Uio	ICT Law	2008 autumn	Inactive	Plan confirmed 1.12.2008	ICTLaw	2008	2008	nothing

Table 4.1 has two students each of them registered twice with University of Oslo. Each time they register, their student names, the study programme and the university name have to be repeated if the data is not organized intelligently. To ensure intelligent organization of the data, the database table 4.1 need to be (normalized) split into two tables consisting of static and dynamic tables. Since the student name, the study programme and the university name are static fields it will be unnecessary and redundant to request for them each time a student want to register for a course. It will also create update problem since modifying the 'Class' field for example will affect only one record instead of two creating inconsistent data. So normalization will be used to separate the dynamic data from the static ones. This is done by assigning unique keys (primary keys) to the statics data. The primary keys are then duplicated in the dynamic database table. The duplicated primary keys in the dynamic database table are called foreign keys. This way only the keys which reference the static data are repeated but the data themselves remain in the static table. The repetition of the keys will save more storage space than the repetition of the entire static data. This is because we use only one field (foreign key) to represent several fields. It will also allow the data controller or data subject to perform further processing with the aid of a key instead of typing or supplying the same personal data again and again.

The normalized tables will now look as follows:

Table 4.2: Static fields

primary key	name	school	Study	Class
101	John Haakon	University of Oslo	ICT Law	2008 autumn
102	Andy Morrison	University of Oslo	ICT Law	2008 autumn

Table 4.3: Dynamic fields

foreign key	Status	Right	dept	fee paid	registration	course
101	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
101	Active	Plan confirmed 13.06.2009	ICTLaw	2009	2009	thesis
102	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
102	Inactive	Plan confirmed 1.12.2008	ICTLaw	2008	2008	nothing

The tables 4.2 and 4.3 represent the separation of table 4.1 into static and dynamic parts. The table 4.2 consists of all fields that will not change regularly and 4.3 consists of all fields that will change regularly. The data in the 4.2 is usually supplied once. Table 4.2 is connected to 4.3 with the aid of primary and foreign keys. This means anytime the foreign keys 101 or 102 is repeated in the 4.3, the database will automatically know that 101 and 102 refer to the static data of John Haakon and Andy Morrison respectively (in table 4.2). With this data organization the number 101 will be used to represent John Haakon's static data in the subsequence data processing.

This could be extend further so that different departments could use the same 101 to access data about John Haakon. Suppose John Haakon want to register for a course in another department, he or the data controller has to add a new entry to table 4.3 and change the entries for the 'dept' and the 'course' fields to the new entries as depicted in the able 4.4 below.

Table 4.4: Dynamic fields

foreign key	Status	Right	dept	fee paid	registration	course
101	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
101	Active	Plan confirmed 13.06.2009	ICTLaw	2009	2009	thesis
101	**Active**	**Plan confirmed 13.06.2009**	**HRLaw**	**2009**	**2009**	**HR001**
102	Active	Plan confirmed 13.06.2008	ICTLaw	2008	2008	privacy
102	Inactive	Plan confirmed 1.12.2008	ICTLaw	2008	2008	nothing

The table 4.4 makes it easy for John Haakon to register for a course in the human right department (HR) without filling a new registration form. All that he has to do is to add a course and change the department name. Instead of starting the whole registration process again in the human right department the ICTLaw department and human right department can easily share data through normalization. Both the human right department and the ICTLaw department will require access to a common database to make this intelligent use of data possible. Better still the departments can be assigned primary and foreign keys in a similar manner as discussed above in order to eliminate the dependance of department on the database organization. This will lead to what is known as third normal form. The levels of consistency designed into a database organization is identify by its normal form. The higher the normal form the less vulnerable it is to inconsistencies and anomalies [39].

If John Haakon's address changes he only has to do it in the static table and it will automatically reflect in other departments because the primary key remains the same.

Thus, instead of allowing each department or unit to keep separate addresses for each data subject, normalization can be used to prevent the redundancy so that the units or the departments can use only one address for their various operations. This helps to ensure data consistency as an address change at one department will automatically reflect in the other departments.

Normalization will help government to spend less time in organizing data when a new department is created from the existing ones or departments are reorganized. There may be no need to merge personal data obtained from the separate departments in order for the a new department to function, because organization of personal data is no longer dependent on departments as a result of normalization.

This is a typical example of intelligent use of data. However, this way of organizing data may be prohibited by the DPD. It may be against the principle of purpose specification . Normalization will allow different departments to access the same data collected for a specific purpose. Since different government departments may have unrelated objectives, such processing may run contrary to the original purpose for which the data was collected. It may therefore not be consistent with the DPD recital 28 and article 6(b) which prohibit re-purposing of data.

Intelligent use of data could facilitate the quality of data in accordance with DPD article 6(d) . Instead of having personal data scattered across government departments, normalization can provide a single data source which can ensure

[39] http://en.wikipedia.org/wiki/Database_normalization#Normal_forms

consistency and accuracy of data. Normalization can ensure that data change at one government department reflect in all departments. The DPD article 6(b) could be an obstacle to intelligent use of data.

This obstacle could be remove if data subject concern is sought during registration process to allow data sharing. This will be consistent with DPD recital 30 and article 7.

4.2.4 Interoperability

Interoperability comes from two words ”inter” and ”operability”. In the computing world it is the ability of two or more incompatible systems to work together. For example the Microsoft operating system should be able to communicate with the Linux operating system. For non computing fields it is the ability of two or more departments, organizations, regions or governments to work together. Interoperability is the ability of two or more organizations to communicate and share information, such as voice, data, images and video [40]. In the i2010 action plan, interoperability is beyond the ”interoperation” between departments and organization within a state but embraces cross-border services for citizens, businesses and public administrations. This means various organs of state and member states should be able to share information such as personal data. Interoperability could ensure secure communications between administrations or cross-border access to resources [41].

To achieve interoperability requires technical schemes which will ensure that personal data can be accessed or shared among departments, organizations and States. There are various schemes available for these possibilities. Among them are, using centralized databases or information system, electronic identification management (eIDM) system and distributed databases or information system. These schemes are referred to as key enablers (see 2.1.4). Database helps to ensure proper storage space management and data retrieval in an information system.

The design schemes for databases determine how data is organized in an information system. For centralization, the database is stored in one location for all authorized users. This means the same database could be shared by dif-

[40] Office Of Domestic Preparedness, http://www.ojp.usdoj.gov/odp/docs/acu_trp1000.pdf. Developing Multi-Agency Interoperability Communications Systems, User's Handbook page 8

[41] Commission of the European Communities. i2010 e-government action plan, accelerating e-government in Europe for the benefit of all. http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id April 2006.

ferent government departments, administrations or governments. An example of an information system that supports centralized database is Schengen Information System (SIS). This is the Schengen states surveillance information system which is used for cross-border surveillance. Information stored in the SIS central database can be accessed by all member states. When information such as wanted or unwanted persons is stored in SIS central database from a state, all the member states will be able to access the information and act accordingly. Other information systems that support centralized databases are Europol, Interpol etc.

Distributed databases or information systems are quite different from the centralized system. Unlike centralization where only one database is kept for universal access, distributed information system mostly requires each department, agency or state to keep a separate database. The information in this separate database is now shared with the aid of middleware software. Middleware is software that allows different computer programs running on different computers to communicate. The main advantage of distributed system over centralized system is that it provides multiple sources of failure and security. This means when one computer is not working the other computer could be relied on for data access. On the other hand, since only one computer is usually used in centralized system, when that computer breaks down or is hacked the entire information system could collapse.

The drawbacks of the distributed system is data consistency. Since there are several computers involved in the distributed system there is the need for consented effort to ensure that information is up to date on all the computers.

The need for interoperability raises privacy concerns in areas such as information quality, information transfer, proportionality, the use of eIDM, repurpose of data and data subject's control issues. Data controllers need to ensure that the information they collect are complete and of high quality.

The data collected should be meaningful with respect to what they are intended to describe, relevant and complete with respect to the purpose for which the data was collected [42]. The DPD article 6(1)d requires that data collected from data subjects should be accurate and kept up to date. This provision could have significant impact on the interoperability requirements of i2010 action plan. This means whatever information system scheme is used in implementing interoperability must ensure that personal data is kept up to date. The easiest way to achieve interoperability and yet keep data up to date is to use a centralized database or information system. This way, only a copy of a person's data will be maintained in the information system. Any change

[42] Lee A Bygrave. Data Protection Law Approaching Its Rationale, Logic and Limits, page 62-69. Kluwer Law International, 2002

made to the personal data will occur at one point. This will ensure quality and consistent information. On the other hand, decentralized or distributed system could have an impact on data consistency. According to DPD article 7(a) the data subject could decide which member state is allowed to process his or her personal data. He could also withdraw the consent when appropriate. When this happens the personal data has to be updated in all the distributed information system. This could be a daunting task and could lead to data inconsistency. In distributed system, communication error could potentially contribute to data inconsistency. If a network error occurs in a part of the information system during transmission part of the information system could be updated while the rest remains outdated.

The design choices of the information system could impact on information quality or data consistency. For example the SIS allows contracting states to keep their own national database which will be out of synch with the centralized SIS database. The information about cross-border security obtained nationally is sent to the central SIS database from time to time. A copy of the information is kept in the national database. When an error occurs during transmission or during information update the information in the national information system will be inconsistent with the central information system. In [43] it was noted that the same search query has to be sent to both the national database and the SIS database because a national search is not only a SIS search, but it involves a search in both the national system and SIS database. Persons not registered in SIS would escape detection because a negative hit in SIS does not necessarily mean that a person is cleared. Searching the national information system or database may reveal other information than the one in the SIS, since a person may be registered in the national system but not in SIS. This means the two databases are not always consistent with each other.

This underscores the potential of data quality problems with such information system and how design choices could have an impact on the privacy of data . Incomplete or inconsistent personal data is a violation of the DPD article 6(1)d. E-government systems which are designed to be accessed across member states could potentially suffer from information quality problems.

Purpose specification is another potential danger to privacy in interoperable e-government system. Personal data has to be collected for a specific purpose and personal data collected for one purpose cannot be processed for other incompatible purpose without the consent of the data subject. The purpose shall be defined, shall be legitimate and further processing of the data collected shall be compatible the DPD recital 28, article 6(1)b.

[43]Stephen Kabera Karanja. The Schengen information system in Austria, an essential tool in day to day police and border control work. Journal of Information, Law and Technology (JILT), 2002

Data sharing could change the original purpose for which data is collected. Normalized databases link a unique key such as a personal number to personal data such as name and street address. Once this is done, different departments and government agencies can use the personal number to access the information without the need to fill a new form since the database is normalized or centralized across the departments or states. Since each department usually has different missions, the retrieval of personal data from a centralized database for use in different departments could lead to re-purposing of data. For instance, information given for tax purposes could also be used for population or election purpose. Thus information given at one government department for a specific purpose could be used for many purposes. This is usually known as proactive services [44]. In Ireland for instance the birth of a second child automatically allows information to be sent to the responsible agency which will trigger child allowance without the parent filling any additional form.

It is convenient not to fill a new form each time you visit a different government department but the practice may violate the DPD article 6(1)(b), 10(b), and 11(b) . Some of these possible violations may be caused by technical design choices and the need for convenience. It is technically convenient, effective and efficient to design such information systems. It however important to note that such data processing may not always lead to the violation of the DPD if it is done fairly and consistent with the original purpose.

The action plan is expected to support cross-border identification (see 2.1.4). This will lead to the development of an eIDM system. The electronic identification system will allow authentication, enabling convenient and secure access to different applications and computer resources across the EU. Under the eIDM system users can use a single login to access e-government resources across the EU. This means either the personal data would be stored in a centralized or distributed information system for processing by member states. In 2003 The Working Party of Data Protection in examining the security risk of Microsoft.NET Passport found that the concentration of data in two big databases posed a serious security risk [45]. This suggests that using distributed database system for eIDM system could help minimize the security risk. However, when personal data is distributed across-borders it will be difficult to ensure proper data subject control as required by directive DPD article 11(c), 12(a). In order for data subjects to be properly assured of information quality they need to acquire the information from all the possible data

[44] Thomas B Riley. E-government vs. e-governance, examining the differences in a changing public sector climate. May 2003 page 159-163

[45] EU Data Protection Working Party. Working document on online authentication services. Technical Report 10054/03/EN WP 68, EU, January 2003 page 11

controllers across the member states. This will put undue burden on the data subject and may not be proportionate.

Interoperability is not always a danger if the necessary conditions exist for such processing. The DPD article 7(b), 7(c) , 7(d) and recital 30, allows such forms of processing if they are necessary. It is however not clear whether this form of data processing that will help government departments and state operations is necessary. This will depend on the interpretation of 'necessary'. In a very strict sense such government operation may not be necessary. Even if the 'necessary' requirement is less stringent, it is not clear if the validity of processing will be proportionate to the original goal of data collection.

4.2.5 Data Security

The risk to data security is increased the moment personal data is put on a network or a form is made available online to collect personal data. The risk is even greater when the network is connected to the Internet. On the Internet, the potential risk of unauthorized access is global. Anyone who has access to the Internet could illegally access personal data if appropriate security measures are not put in place.

The security of personal data stored online will require a proper password scheme to allow future retrieval of the information online. It will require encryption to protect the data during transmission from the data subject to the data controller. Spam is one of the security threats to privacy. Spam is unsolicited e-mail sent from anonymous individual or businesses to a person usually for marketing purposes, without the consent of the person. Spam can also be used for a denial of service (DOS) attack, or e-mail borne attack on an ISP or an enterprise e-mail system. For this purpose bulk e-mail is sent to the e-mail server of an ISP in attempt to slow or shut the server down all together. The basic spam input is the e-mail address transmitted over the Internet. The spammers collect the e-mail addresses during data transmission online and use them to spam their victims. Though the e-mail address could be revealed from many sources online, e-government cannot be an exception. It was found in [46], that between 1 July and December 2005 spam made up 50% of all monitored e-mail traffic with annual average of 68.6%. The EC's Technical report noted that the number of e-mail-borne attacks on businesses have increased from an insignificant figure to 2-3 targeted attacks per week during 2005.

The relevant of spam to privacy may depend on whether it is likely to iden-

[46] European Commission Information Society and Media Directorate General. Statistical data on network security, page 3-8. Technical report, Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: BU29 03/41, march 2007

tify an individual with his or her e-mail. Since spammers spam with e-mail without authorization such use may violate the provisions of the data protection directive if e-mails are regarded as personal data. Whether or not an e-mail is a personal data will depends on the interpretation of personal data. According to the DPD article 2a, personal data is any information relating to a data subject. The data should directly or indirectly relate to the natural person or to his identification number, physical, physiological, mental, economic, cultural or social identity. The extent of such a relationship shall be understood as a less stringent one, the DPD recital 26. The slightest possible relationship between data and data subject may make the data personal. There should be a reasonable way in establishing this relation. Cost, time and energy spent in relating data to a natural person or a natural person to data either directly or indirectly determines the degree of reasonability. Information per se has no relevance if it has no likely reasonably means of relating to a data subject (an identified individual).

This means an auxiliary information such as e-mail may qualify as personal data if the auxiliary data relates to an individual. It is possible to indirectly relate e-mail to an individual if there is readily available automated databank or additional data. If there is no readily available directory for lookup or any such means, e-mails may be irrelevant for identification since it will not relate to any identified individual. Also e-mails usually contain names of individuals which could make it easy to relate it to an individual.

Phishing is also another important area of network security. Phishing is a means of acquiring sensitive information such as user name, password or credit card information, by masquerading as a trustworthy entity in an electronic communication [47]. Unsuspecting users can be redirected to a fake equivalent of original site through phishing. When the password and user name is obtain through phising they could be used to obtain additional information which could be personal. For instance an the password and user name to someone's e-mail account is obtained through phising it can be used to know the phone number, address, data of birth and other personal data since they are usually accessible from the in box. According to the EU security report, phishing continues to be a great security threat. It accounts for 1 in every 304 of all email transactions since 2005, about 200% rise of the 2004 figure.

Another security risk to e-government is malware attacks. Malware can expose confidential information on a compromised computer. Malware can damage computer without the owner of the computer being aware. In 2004 nearly 80% of home personal computer (PC) were infected by malware and 2.8% of scanned emails in 2005 contained malware. Cyber attacks are rising

[47] Wikipedia. Phishing. http://en.wikipedia.org/wiki/Phising

over 20% per annum.

On the impact of intrusion, the report noted that 68% of organizations has experienced at least one intrusion in 2004 and 88% anticipate an increase in intrusion during 2005.

On the surface the provisions of DPD article 17 is reassuring since it will burden the data controllers with the obligation to make adequate security provision for personal data. The DPD article 17 ensures that the data controller protects personal data from the risk of transmission in cyberspace. However, what is not clear is what level of security is adequate? There is no specific security standard or practice specified in the provision. Considering the level of sophistication of the cyberspace attack adequate security will only encourage ad hoc security measures which are usually not up to the task. A standard security measure will ensure proper security and promote transparency. The data subject will know what is in place for security. This will go a long way to minimize the security fears data subject have for e-government. Network security and privacy concerns were significant in the low e-government patronage. 30-40% of users surveyed cited network security and privacy concerns as the cause of the low patronage in the i2010 midterm review report [48]. There are security standards and best practices such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27033, the Guide to the Assessment of IT risk (GAIT), enhanced Telecom Operations Map (eTom) and Information Technology Infrastructure Library (ITIL) which provide specific security guidelines capable of withstanding the sophistication of cyberspace attack.

Online security has three main components:

- the security at the data subject's end,
- the security at the data controller's and
- security between the two ends.

Each of these three areas needs adequate protection to ensure the security of personal data. The e-government policy is likely to increase the number of citizens who will own and run their own PC online. Since many users lack adequate protection on their home PCs according to European Commission

[48]Statistical Data On Network Security, page 3-8, European Commission Information Society and Media Directorate-General, 2007, Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel- Belgium - Office: BU29 03/41, ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/statistics-network-security-050307_en.pdf

Information Society and Media Directorate report, [49], it is not clear if it is proportionate for data subjects, to be subjected to the requirement of owing and making their home PCs available online without the skills necessary to protect them. The all inclusive policy (see 2.1.1), is likely to put about 30% of EU citizen or data subject at risk of online attack if they are not provided with the necessary skills.

Vulnerable citizens do not only need security from the data controller or processor end or between the transmission lines where data travels but also at the data subject's end. Therefore some of the requirements of the eInclusive would not be proportionate if government does not take an active part to ensuring that vulnerable users acquire the adequate skills needed to protect them from intrusion. The "no citizen left behind" policy recognizes the need for ICT skill. The policy notes that ICT skills is the core for it successful implementation. The policy will ensure that those with no ICT skill acquire the necessary skill. This may include network security and all the basic security knowhow necessary to maintain a home PC online. If this policy is implemented effectively, it will help ensure effective privacy protection when using e-government services. ICT skills are recognized as one of the 52 benchmark indicators in RAND's report (see [50]). This goes to confirm how important ICT skills is to the i2010 action plan.

One of the greatest security threats which is often overlooked is the internal security. With today's level of sophistication a small memory stick could be used to carry unprecedented amount of data which could be detrimental to data subjects and the organization. Employees could reveal, steal or access personal data without proper authorization. In the case of R v Rooney 2006 EWCA crim 1841, Rooney was convicted for disclosing the name of the town R was leaving to her sister. Rooney was an employee of a human resources department of a police constabulary, where she had access to the personal data of other employees. The prosecution argued that the defendant had abused her position and breached the Data Protection Act 1998 ("DPA") by accessing personal information that was not related to her work and then passing it on to someone without consent [51].

[49] European Commission Information Society and Media Directorate- General. Statistical data on network security, page 3-8. Technical report, Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: BU29 03/41, march 2007

[50] Irma Graafland-Essers and Emile Ettedgui. Benchmarking e-government in Europe and the US, page 10. RAND, 2003

[51] R v Rooney. CASETRACK, http://www.casetrack.com/ct4plc.nsf/items/6-203-6631, 2006.

4.3 Does the i2010 Plan Shows Strong Privacy Concerns?

The i2010 action plan does not explicitly emphasize on privacy. However, in the "no citizen left behind" policy, the phrases *"...citizens benefit from **trusted**, innovative services.. . "* and *"... eIDM ... complying with data protection regulations"* used to describe the nature of services to be provided and the nature of the electronic identification management (eIDM) system. In report found in [52], which is an extensive exposition of the i2010 policy, does not raise any privacy concerns. It rather focuses on the issue of identification and authentication in the key enabler policy section. Privacy is not given much prominence. Furthermore, the issue of "trust" was not expanded in the section 2 of the action plan.

Moreover, making "efficient and effective public services delivery a reality" policy objective of the i2010 action plan does not make mention of privacy. This policy objective requires benchmarks on how the efficiency and effectiveness of e-government system can be measured. Various indicators has been developed as a results of this policy objective, however, among the 52 benchmark indicator there is no attempt to quantify privacy [53]. There is no mention of privacy impact assessment in fulfillment of the accountable e-government policy objective expressed in this section. The requirement for effectiveness in that policy objective includes high user satisfaction, transparency and accountability.

The brief use of "trusted" in the "...trusted innovative services" in the policy objective of the action plan seems to indicate the significance of privacy and security concerns. Though the recognition of trust in this document is an important step in ensuring properly functioning and accountable e-government information system it does not go far enough to illuminate their significance. Trusted e-government systems are an essential ingredient in boosting citizens' confidence and therefore it cannot be taken lightly.

Ironically, comparing this action plan to that of US, the US has a clear and vivid policy on privacy. In the e-government Act Section 208 Implementation Guidance of US, privacy is explicitly expressed as one of the prominent requirement for e-government system. There is a clear privacy policy and requirements. These include privacy impact assessment policy objective, post

[52] European Commission-Directorate General Information Society and Media. ICT for government and public services. http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

[53] Commission of the European Communities. Preparing Europes digital future i2010 Mid-Term Review, volume 3 of COM(2008) 199 final. EC, April 2008.

privacy assessment policy objective and privacy translation policy objective [54].

This disparity could be attributed to the value the US places on privacy in case of e-government. Or the fact that privacy is sector specific and requires more detailed policy than that of the EU which relies on comprehensive laws or directives. Also the disparity in the level of trust US and EU citizens have for their respective governments could influence the rather strong privacy concerns by the US government. US citizens usually dislike government backed regulations so the assurance of trust is necessary to ensure successful implementation of e-government system.

In addition, the disparity could also be informed by the main goal of the policy plans. Though the i2010 action plan somehow expresses privacy and security, it seems to place more emphasis on the economic benefit of e-government than trusted e-government system. The lack of strong privacy concern could also be attributed to the general disregard for privacy in European e-government system as noted by Xavier Huysmans [55].

It could also be attributed to the fact that the EU has working party established by DPD article 29 to oversee the impact of technological advancement such as e-government on privacy. Over the years the working party has taken up the responsibility of investigating various privacy infringements instigated by technological innovation. The most relevant to this thesis is the Microsoft.NET passport investigation [56]. A number of recommendations were made in this report which could help shape the privacy policy regarding the use of eIDM in e-government systems across the EU.

4.4 The Need for Privacy Impact Assessment

The need for privacy impact assessment will depend on the value of privacy to e-government system. The success of e-government may be linked to how privacy fears are alleviated. Privacy is one of the factors that affect the patronage of e-government. In 2003, a report published by RAND Europe partly dwelled on the importance and impact of privacy on e-government. According to the report, e-government services which require users to reveal less personal information enjoyed greater patronage than those which require great deal of

[54] Office Of Management and Budget. e-government act section 208 implementation guidance. http://www.whitehouse.gov/omb/memoranda_m03-22/, Feb 2006

[55] Xavier Huysmans. Privacy-friendly identity management in e-government. SpringerLink, http://www.springerlink.com/content/a34758h15j085420/fulltext.pdf?page=1

[56] EU Data Protection Working Party. Working document on online authentication services. Technical Report 10054/03/EN WP 68, EU, January 2003

personal information[57]. Five years down the line there has not been much significant change in the e-government patronage across the EU. Many of the factors that affect e-government patronage seem unaddressed.

The midterm e-government country review report released in April 2008 depicts low e-government patronage [58]. The report presented the results of 52 e-government benchmark indicators which were set up by the Commission in co-operation with Member States. This is in accordance with the i2010 benchmark framework endorsed by the i2010 High Level Group in April 2006. The country profile report shows general rise in the availability of e-government services but a stagnant process in the patronage of these services. Austria is one of the high performing countries in this report with 100% basic public services fully available online. Unfortunately the patronage of these services saw a sharp decline from 33% to 27% between 2006 and 2007. Comparing the 2007 figure to the population of Internet users, more than 50% of the citizens do not use e-government services. Belgium has 63% Internet users but as at 2007 only 23% of the Internet users were e-government service users.

Norway was ranked as one of the top performing States. 26% of Norwegians used e-government services to send filled in forms. This is twice the European average. 57% out of 77% of regular Internet users used e-government services. It recorded 5% rise of users between 2006 and 2007.

In general an average of 13% used e-government services to send filled in forms and not more 35% of Internet users in the Member States patronized e-government services according to the report.

There are many factors such as privacy, security, trust that could contribute to this slow pace of patronage as outlined in the RAND report [59]. . Trust may composition of privacy and security concerns . Lack of security and privacy could have negative impact on the e-government patronage. Convenience on the other hand could impact positively on e-government patronage. Convenience usually overrides the need for privacy and is likely to increase e-government patronage. According to the RAND Europe report, "*The attitudes of citizens toward e-government point to convenience of time and location as factors that strongly favor e-government over traditional government*".

Although the reasons for this low patronage was not cited in the i2010 midterm country review report the impact of privacy and other factors such as

[57]Irma Graafland-Essers and Emile Ettedgui. Benchmarking e-government in Europe and the US, page 10. RAND, 2003

[58]Commission of the European Communities. Preparing Europes digital future i2010 Mid-Term Review, volume 3 of COM(2008) 199 final. EC, April 2008

[59]Irma Graafland-Essers and Emile Ettedgui. Benchmarking e-government in Europe and the US, page 10. RAND, 2003

convenience on the patronage of e-government services cannot be underestimated. In [60] the report revealed that there seem to be decreasing use of e-government services. Network security and privacy concerns were significant in the low patronage. 30-40% of users surveyed cited network security and privacy concerns as the cause of the low patronage. It is therefore quite uncertain why privacy impact assessment was not recognized as part of the 52 performance indicators. The impact of privacy on the patronage of e-government services requires proper consideration since it has the potential of improving the patronage.

[60] Statistical Data On Network Security, page 3-8, European Commission Information Society and Media Directorate-General, 2007, Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel- Belgium - Office: BU29 03/41, ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/statistics-network-security-050307_en.pdf

Chapter 5

Conclusion

E-government has come to stay and future public administration cannot do without it. There is no doubt that privacy will play a significant role in ensuring proportionality and in regulating the power balance between citizens and states. To a large extent privacy will contribute to the level of e-government patronage and eventual success of the i2010 program. For that matter strong privacy concern is required to alleviate all fears regarding misuse of personal data. For this to be fulfilled, there should be explicitly policy guidelines on how privacy issues should be handled in e-government. This will reassure the participants of the e-government system. It is observed that the policy does not show strong privacy concerns. The approach to privacy in the i2010 action plan could not ensure proper balance of power between individuals and states. There are no clear policy guidelines as to how privacy and data protection should be implemented in e-government system. Lack of privacy impact assessment for the plan gives an indication of less regards for privacy in the plan. It is observed that the US plan has comprehensive privacy plan for e-government and that could reassuring data subject and boost e-government patronage.

The DPD will go a long way to reassure data subjects of protection against online security risk. It put the responsibility on the data controller to ensure that proper security provisions are made to protect personal data. However the adequacy security requirement is not transparent enough to alleviate privacy fears. By adopting standard security practices or standards would help minimize privacy fears and fulfill the objectives of adequate security. It is also significant to note that DPD article 17 does not cover or protect data subject's home PC. Since home PCs suffer greatly from security threats it is important for government to support programs that will aid vulnerable data subject who otherwise would not rely on home PC to engage.

government online. This will be proportionate and will help to reassure the data subject of total security and also enhance patronage. The issue of informational quality could be solved with robust information system capable of with stand network or communication error. Such system should not collapse when communication error occur but be able to continue trying the update process until it is successful. In case online live update is not possible, there should be effective way of doing offline update in order to ensure information quality.

Finally, data protection provision will be greatest obstacles to interoperability in the e-government action plan. In many respect interoperability requirement could violate some of the provisions of DPD. Interoperability is a key to the i2010 action plan policy objectives. Provisions such as data subject control, re-purposing of data, fairness and identification could impact on how interoperability is achieved in e-government. This means the design choices need to consider the effect of these obstacles in order to meet the requirements of DPD. We observed that this could be achieved at the expense of technical efficiency and effectiveness, and data subject convenience. For this to be avoided there is a need to revise certain aspect of the Directive that is inimical to achieving the all important goal of interoperability. There must be a careful balance in order not to dispossess the data subject of the right to privacy.

Also a comprehensive e-government legislation that seeks to address the privacy barrier to e-government may be necessary to the meet the important requirements of i2010 action plan. This will be consistent with the examples set by Austria, the Czech Republic, Finland, Italy, Latvia, Slovakia and, recently, France [61]. In doing so, we need to ensure a careful balance between strong privacy protection and the need to meet the requirements of the i2010 action plan in order not to erode public trust in e-government.

[61] Breaking Barriers to eGovernment, Overcoming obstacles to improving European public services Modinis study Contract no. 29172 http://www.egovbarriers.org/downloads/deliverables/1b/A_Legal_and_Institutional_Analysis_of_Barriers_to_eGovernment.pdf page 32

Bibliography

1. European Commission. Guidelines for improving the synergy between the public and private sectors in the information market.

http://www.viw.or.at/intern/riand4.pdf, April 2006.

2. Jean Monnet Professor Antonio Alabau. Understanding the e-government policy of the european union, pages 8-9. http://ec.europa.eu/idabc/servlets/Doc?id=18443, July 2003.

3. Professor Dag Wiese Schartum. Access to government held information, challenges and possibilities. http://www.viw.or.at/intern/riand4.pdf, February 1998.

4. Lawrence Lessig. Code 2.0, volume 2. Basic Books, 2 edition, December 2006.

5. Daniel E Smith. The right to privacy,the rights and liberties under the law. http://www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/glenn404.htm, April 2004.

6. David Bender and Larry Ponemon. Binding corporate rules for crossborder data transfer. Rutgers Journal of Law and Urban Policy, 3:2, 2006.

7. Janine S Hiller. Privacy strategies for electronic government. Center for Global Electronic Commerce Pamplin College of Business Virginia Polytechnic Institute and State University, January 2001.

8. Eu data protection directive

http://www.cdt.org/privacy/eudirective/EU_Directive_.html, 1995.

9. Yue Liu. The principle of proportionality in biometrics:case studies from norway. Computer Law and Security Review, 25:237-250, 2009.

10. R v rooney. http://www.casetrack.com/ct4plc.nsf/items/6-203-6631, 2006.

11. Electronic Privacy Information Center and Privacy International. Privacy and Human Right 2002, An International Survey of Privacy Law and Development, volume 1. Butterworths, 13 edition, 2002.

12. Edward J Bloustein Stanley I Benn. Philosophical dimensions of privacy, An Anthology. Cambridge University Press, 1984.

13. Ronald Leenes Bert-Jaap Koops. Code and the slow erosion of privacy. 12 Mich. Telecomm. Tech. L. Rev., 115, 2005.

14. Council of Europe The European Convention on Human Rights. ROME

4 November 1950 and its Five Protocols, STRASBOURG 20 January 1966. EU, January 1966.

15. Wikipedia. Positive obligation.

16. Oliver Sanders. Using article 8 rights to access and protect personal or private information.

17. Yutaka Arai-Takahashi. Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR, page 3-10. Intesentia, 2002.

18. ECJ. Judgement in the case between peck v united kingdom.

http://www.echr.coe.int/eng/Press/2003/jan/Peckjudeng.htm, January 2003.

19. ECJ. Case of niemietz vs germany. http://www.bagger-tranberg.dk/EU-ret/Filer_homepage/Niemietz_vs_Germany.pdf, December 1992.

20. Lee A Bygrave. Data Protection Law Approaching Its Rationale, Logic and Limits. Kluwer Law International, 2002.

21. ICO. The durant case and its impact on the interpretation of the data protection act 1998. , Feb 2006.

22. Judgement strasbourg, i v finland . http://www.cl.cam.ac.uk/ rja14/Papers/echr-finland.pdf, 2008.

23. P Shears and G Stephenson. JamesIntroduction to English Law, volume 13. Butterworths, 13 edition, october 1996.

24. Thomas B Riley. E-government vs e-governance, examining the differences in a changing public sector climate. May 2003.

25. US Government. E-government act of 2002. http://frwebgate.access.gpo.gov/cgi-bin/getdoc. cgi?dbname=107_cong_public_laws&December 2002.

26. Commission of the European Communities. i2010 egovernment action plan, accelerating egovernment in europe for the benefit of all.

http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id

April 2006.

27. European Commission-Directorate General Information Society and Media. Ict for government and public services.

http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

28. Corien Prins. E-government, a comparative study of the multiple dimensions of required regulatory change. 11, December 2007.

29. Office Of Management and Budget. Egovernment act section 208 implementation guidance. http://www.whitehouse.gov/omb/memoranda_m03-22/, Feb 2006.

30. Irma Graafland-Essers and Emile Ettedgui. Benchmarking e-Government in Europe and the US. RAND, 2003.

31. Commission of the European Communities. Preparing Europes digital future i2010 Mid-Term Review, volume 3. April 2008.